Kezdés ideje	2023. május 10., szerda, 11:07
Állapot	Befejezte
Befejezés dátuma	2023. május 10., szerda, 11:52
Felhasznált idő	45 perc 27 mp
Pont	Még nincs lepontozva

1 kérdés

Hibás

0,00/1,00 pont

Adott a következő mátrix, amelynek második sorát úgy kell megválasztania a lehetőségek közül, hogy egy lineáris kód generátormátrixát kapjuk.

Ha ezt megtette, akkor válaszoljon a következőkre:

ez a mátrix [3] ✖ hosszúságú kódhoz rendel hozzá redundáns kódokat.

1 0 0 1 0 1

[0 1 0 1 0 1] ✖

0 0 1 1 1 0

[0 1 0 0 1 1] [0 1 1 0 1 1]

[6]

Válasza helytelen.

A helyes válasz:
Adott a következő mátrix, amelynek második sorát úgy kell megválasztania a lehetőségek közül, hogy egy lineáris kód generátormátrixát kapjuk.

Ha ezt megtette, akkor válaszoljon a következőkre:

ez a mátrix [6] hosszúságú kódhoz rendel hozzá redundáns kódokat.

1 0 0 1 0 1

[0 1 0 0 1 1]

0 0 1 1 1 0

MOODLE | ÓBUDAI EGYETEM

Kérdések elküldve, katt az elküldött

1,00/1,00 pont

Az RSA [nyilvános] ✔ kulcsú rejtjelezés vagy titkosítás, más néven [aszimmetrikus] ✔ kulcsú titkosítás egy olyan kriptográfiai eljárás neve, ahol a felhasználó egy kulcspárral rendelkezik. A [titkos] ✔ kulcs titokban tartandó, míg a [nyilvános] ✔ kulcs széles körben terjeszthető. A kulcsok matematikailag összefüggnek, ám a [titkos] ✔ kulcsot gyakorlatilag nem lehet meghatározni a [nyilvános] ✔ kulcs ismeretében. Egy, a [nyilvános] ✔ kulccsal kódolt üzenetet csak a kulcspár másik darabjával, a [titkos] ✔ kulccsal lehet visszafejteni.

nyilvános | titkos

szimmetrikus

Válasza helyes.

A helyes válasz:
Az RSA [nyilvános] kulcsú rejtjelezés vagy titkosítás, más néven [aszimmetrikus] kulcsú titkosítás egy olyan kriptográfiai eljárás neve, ahol a felhasználó egy kulcspárral rendelkezik. A [titkos] kulcs titokban tartandó, míg a [nyilvános] kulcs széles körben terjeszthető. A kulcsok matematikailag összefüggnek, ám a [titkos] kulcsot gyakorlatilag nem lehet meghatározni a [nyilvános] kulcs ismeretében. Egy, a [nyilvános] kulccsal kódolt üzenetet csak a kulcspár másik darabjával, a [titkos] kulccsal lehet visszafejteni.

3 kérdés

Részben helyes

0,75/1,00 pont

Adja meg a titkosítási eljárások típusát!

DES	szimmetrikus kulcsos	✔
RSA	nyilvános kulcsos	✔
Rijndael	nyilvános kulcsos	✖
AES	szimmetrikus kulcsos	✔

Válasza részben helyes.

Jól választott ki: 3.
A helyes válasz:
DES → szimmetrikus kulcsos,

RSA → nyilvános kulcsos,

Rijndael

→ szimmetrikus kulcsos,
AES → szimmetrikus kulcsos

1,00/1,00 pont

Mely titkosítási eljárások fedik (fedhetik) el az árulkodó nyelvi statisztikákat?

- [ ] Vigenère-rejtjel
- [ ] Ceasar eljárás
- [x] Rijndael ✔
- [x] RSA ✔

Válasza helyes.

A helyes válaszok:
RSA,

Rijndael

5 kérdés

Helyes

1,00/1,00 pont

Adott a fenti séma és jelölésrendszer egy lineáris kódolási eljárás esetében.

Rendezze sorba kapcsolódó szindróma-dekódolás lépéseit:

- ✔ A V vett szónak megfelelő S szindróma kiszámítása.
- ✔ Az S-nek megfelelő E hibavektor kiolvasása a dekódolási táblázatból.
- ✔ A C'=V-E kód számítása.
- ✔ U' megadása C' alapján.

Válasza helyes.

1,00/1,00 pont

Érvényes továbbított kódszóban t hiba javításához ilyen Hamming távolságú kódhalmazt kell használni (írja le a matematikai kifejezést).

Válasz: 2t+1 ✔

A helyes válasz: 2t+1.

7 kérdés

Helyes

1,00/1,00 pont

Azt az eljárást, amely az illetéktelen kódolvasók által az átvitel során elkövetett aktív vagy passzív támadások ellen véd így nevezzük (írja le a választ):

Válasz: titkosítás ✔

A helyes válasz: titkosítás.

8 kérdés

Helyes

1,00/1,00 pont

Legyen adott a következő kódrendszer (az előző kérdésből):

x1: 0011111,

x2: 0011110,

x3: 0100101,

x4: 0100011

A kódrendszer nem hibajavító.

Igaz vagy hamis az állítás?

Válasszon ki egyet:

- (●) Igaz ✔
- ( ) Hamis

A helyes válasz az 'Igaz'.

1,00/1,00 pont

Elegendő minden esetben az eredeti üzenet kódszavához még egyszer hozzáírni a kódszavat a folytatásban ahhoz, hogy kijavíthasuk a hibás továbbítást.

Válasszon ki egyet:

- Igaz
- Hamis ✔

A helyes válasz a 'Hamis'.

10 kérdés

Helyes

1,00/1,00 pont

A kódokat *n* hosszúságú vektorokként értelmezzük.
- Legyen M a forráskód-szavak halmaza (2^k van belőlük)
- *n* a kiterjesztett kódszavak hossza
- *d* a megadott kódhalmaz Hamming távolsága

Ennek alapján a blokkkódot általában a következő rendezett hármas jelöli: (n, M, d).
Azokra a blokkkódra, amely legfeljebb t hibát javíthat igaz a következő:

$$M \cdot \sum \binom{n}{i} \leq 2n$$

Igaz vagy hamis az állítás?

Válasszon ki egyet:

- Igaz
- Hamis ✔

A helyes válasz a 'Hamis'.

1,00/1,00 pont

Azokat a blokk kódokat, amelyek kielégítik az (n,M,d) kódhalmazban a Hamming egyenlőtlenséget (azaz a Hamming korlátot), így nevezzük:

Válasszon ki egyet:

- tökéletes kód ✔
- redundáns kód
- lineáris kód

Válasza helyes.

A helyes válasz: tökéletes kód.

12 kérdés

Helyes

1,00/1,00 pont

Az a kód, amely *m* adatbitet, (az eredeti üzenet kódját), és további *r* redundáns bitet (vagy ellenőrző bitet) tartalmaz

Válasszon ki egyet:

- bináris blokk kód ✔
- Huffman kód
- szisztematikus kód

Válasza helyes.

A helyes válasz: bináris blokk kód.

1,00/1,00 pont

Mit nevezünk a kódszavak távolságának?

Válasszon ki egyet:

- az egyesek számát a bináris kódszavakban
- a kódszavak hossza közötti különbséget
- azonos hosszúsági bináris kódszavak eltérő bitjeinek a számát✔

Válasza helyes.

A helyes válasz: azonos hosszúsági bináris kódszavak eltérő bitjeinek a számát.

14 kérdés

Helyes

1,00/1,00 pont

A kódoláselméletben az a hibajavító kód, amelynél a kódszavak bármilyen lineáris kombinációja szintén kódszó

Válasszon ki egyet:

- kombinációs kód
- komplex kód
- lineáris kód✔

Válasza helyes.

A helyes válasz: lineáris kód.

15 kérdés

Helyes

1,00/1,00 pont

Mi ez?

Valamely bitvektorhoz rendelt redundáns bit, amely a bitvektor átvitelénél a vevőoldalon hibajelzést tesz lehetővé. Értéke 0 vagy 1, amely attól függ, hogy a bitvektor összege páros vagy páratlan. Ennek a bitnek a neve

Válasszon ki egyet:

- záróbit
- páros bit
- paritásbit✔

Válasza helyes.

A helyes válasz: paritásbit.

1,00/1,00 pont

Mire szolgálnak a redundáns bitek a kódolás alkalmával?

Válasszon ki egyet vagy többet:

- [x] a hibafelismerést szolgálja
- [x] a megfelelő kódtávolság biztosításához
- [ ] a tömörítés visszafejtését szolgálja

Válasza helyes.

A helyes válaszok:
a megfelelő kódtávolság biztosításához,
a hibafelismerést szolgálja

17 kérdés

Helyes

1,00/1,00 pont

A távközlési rendszer mely részén áll fenn a támadás veszélye a leggyakrabban?

Válasszon ki egyet:

- ( ) a forrásnál
- (•) a csatornában
- ( ) a vevőnél

Válasza helyes.

A helyes válasz: a csatornában.

1,00/1,00 pont

Melyik tömörítési eljárás alkalmaz kódtáblát?

Válasszon ki egyet:

- futamhossz
- LZ78 ✔
- MPEG

Válasza helyes.

A helyes válasz: LZ78.

19 kérdés

Helyes

1,00/1,00 pont

„Számos különféle transzformációt vizsgáltak az adatok tömörítésére, néhányat kifejezetten erre a célra találtak ki. Például a Karhunen-Loeve transzformáció biztosítja a lehető legjobb tömörítési arányt, de ezt nehéz végrehajtani. A Fourier-transzformáció könnyen használható, de nem nyújt megfelelő tömörítést. Jellemző algoritmusa a diszkrét koszinusz transzformáció . ”

Mely tömörítési eljárásra jellemző a fenti idézet?

Válasszon ki egyet:

- LZW
- JPEG ✔
- MPEG

Válasza helyes.

A helyes válasz: JPEG.

MOODLE | ÓBUDAI EGYETEM

0,60/1,00 pont

Kérdések elküldve, katt az elküldött

Állítsa helyes sorrendbe az RSA kulcs-alkotásának lépéseit!

- ✔ Véletlenszerűen válasszunk két nagy prímet, p-t és q-t.
- ✖ Számoljuk ki az Euler-féle f függvény értékét N-re: f(N)=(p-1)(q-1)
- ✖ Számoljuk ki az N=pq szorzatot. N lesz a modulusa mind a nyilvános, mind a titkos kulcsnak.
- ✔ Válasszunk egy olyan egész számot, e-t melyre teljesül, hogy 1<e <f(N) , és e és f(N) legnagyobb közös osztója 1. Azaz lnko(e, f(N))=1. e-t nyilvánosságra hozzuk, mint a nyilvános kulcs kitevőjét.
- ✔ Számítsuk ki a d számot úgy, hogy a következő kongruencia teljesüljön.
de azonosan egyenlő 1-gyel (mod f(N)), azaz de=1+kf(N) valamely k pozitív egészre. A d számot tiokban tartjuk, ez lesz a titkos kulcs kitevője.

Válasza részben helyes.

Grading type: Absolute position

Grade details: 3 / 5 = 60%

Here are the scores for each item in this response:

1. 1 / 1 = 100%
2. 0 / 1 = 0%
3. 0 / 1 = 0%
4. 1 / 1 = 100%
5. 1 / 1 = 100%

The correct order for these items is as follows:

1. Véletlenszerűen válasszunk két nagy prímet, p-t és q-t.
2. Számoljuk ki az N=pq szorzatot. N lesz a modulusa mind a nyilvános, mind a titkos kulcsnak.
3. Számoljuk ki az Euler-féle f függvény értékét N-re: f(N)=(p-1)(q-1)
4. Válasszunk egy olyan egész számot, e-t melyre teljesül, hogy 1<e <f(N) , és e és f(N) legnagyobb közös osztója 1. Azaz lnko(e, f(N))=1. e-t nyilvánosságra hozzuk, mint a nyilvános kulcs kitevőjét.
5. Számítsuk ki a d számot úgy, hogy a következő kongruencia teljesüljön.
de azonosan egyenlő 1-gyel (mod f(N)), azaz de=1+kf(N) valamely k pozitív egészre. A d számot tiokban tartjuk, ez lesz a titkos kulcs kitevője.

1,00/1,00 pont

Közismert, hogy ha a 0 és 1 eredeti kódszavakat a C = {000,111} kódrendszerbe vezetjük át, akkor a következőképpen dekódoljuk az esetlegesen hibával érkező bináris vektorokat (válassza ki a megfelelőt):

011	1	✔
010	0	✔
110	1	✔
000	0	✔
100	0	✔
001	0	✔

Válasza helyes.

A helyes válasz: 011 → 1, 010 → 0, 110 → 1, 000 → 0, 100 → 0, 001 → 0

22 kérdés

Részben helyes

0,86/1,00 pont

Legyen adott egy kódhalmaz:

x1: 0011111,

x2: 0011110,

x3: 0100101,

x4: 1100011

Párosítsa a következő kódtávolságokat!

d(x2,x4)	6	✔
d(x1,x3)	5	✖
A teljes kód *d* távolsága	1	✔
d(x1,x2)	1	✔
d(x1,x4)	5	✔
d(x3,x4)	3	✔
d(x3,x4)	3	✔

Válasza részben helyes.

Jól választott ki: 6.

A helyes válasz: d(x2,x4) → 6, d(x1,x3) → 4, A teljes kód *d* távolsága → 1, d(x1,x2) → 1, d(x1,x4) → 5, d(x3,x4) → 3, d(x3,x4) → 3

0,33/1,00 pont

Adja meg a tömörítés típusát!

Huffman	veszteségmentes ✔
LZW	veszteséges ✖
JPEG	veszteségmentes ✖

Válasza részben helyes.

Jól választott ki: 1.
A helyes válasz: Huffman → veszteségmentes, LZW → veszteségmentes, JPEG → veszteséges

24 kérdés

Helyes

1,00/1,00 pont

A teljes kódrendszer távolsága

Válasszon ki egyet:

- a kódrendszer kódszavai közötti távolságok minimuma ✔
- a kódrendszer kódszavai közötti távolságok átlaga
- a kódrendszer kódszavai közötti távolságok maximuma

Válasza helyes.

A helyes válasz: a kódrendszer kódszavai közötti távolságok minimuma.

25 kérdés

Helyes

1,00/1,00 pont

Legyen a forrásüzenet halmaza két szó, 0 és 1. Ahhoz hogy egyértelműen (hiba nélkül) visszafejthessük a megérkezés után az üzeneteket a következőképpen kell redundáns kódokkal kibővíteni az eredeti üzenet-szavakat (jelölje az elegendő bővítést):

Válasszon ki egyet:

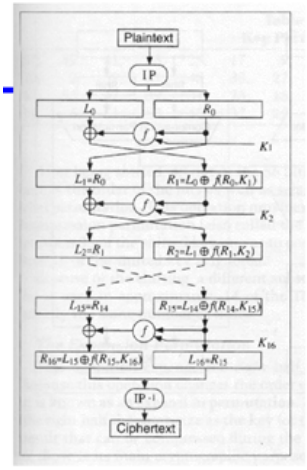
- 0 helyett 0000 és 1 helyett 1111
- 0 helyett 00 és 1 helyett 11
- 0 helyett 000 és 1 helyett 111 ✔

Válasza helyes.

A helyes válasz: 0 helyett 000 és 1 helyett 111.

1,00/1,00 pont

Mely eljárás algoritmusa látható a képen?



Válasszon ki egyet:

- DES ✔
- RSA
- helyettesítő algoritmus

Válasza helyes.

A helyes válasz: DES.

27 kérdés

Helyes

1,00/1,00 pont

Ha tudjuk, hogy a 0 és 1 kódszavakat a C={000,111} kódhalmazba átvezető kód egy lineáris blokkkód, és ezáltal érvényben vannak a következő egyenlőségek:

[0 0 0] = [0] [1 1 1] és [1 1 1] = [1] [1 1 1]
akkor megállapíthatjuk, hogy a kódolási folyamat generátor mátrixa/vektora

Válasszon ki egyet:

- [111] ✔
- [000]

Válasza helyes.

A helyes válasz: [111].

1,00/1,00 pont

Az érvényes továbbított kódszóban *t* hiba észlelése érdekében olyan kódot kell használni, amelynek Hamming távolsága

Válasszon ki egyet:

- 2t+1
- 2t-1
- t+1 ✔

Válasza helyes.

A helyes válasz: t+1.

29 kérdés

Helyes

1,00/1,00 pont

A *d* Hamming távolságú kódrendszer legfeljebb *t* hibajavító akkor és csak akkor, ha

Válasszon ki egyet:

- d=2t+1
- d>2t+1
- d>=2t+1 ✔

Válasza helyes.

A helyes válasz: d>=2t+1.

1,00/1,00 pont

Az a kód, amelyben az *r* redundáns bitet kizárólag a megfelelő eredeti üzenet *m* adatbitjénekn függvényében számítják ki (vagy egy táblázatból egy előre meghatározott algoritmus szerint)

Válasszon ki egyet:

- a szisztematikus kód
- a bináris blokk kód ✔
- a Huffmann kód

Válasza helyes.

A helyes válasz: a bináris blokk kód.

31 kérdés

Kész

3,00 pont szerezhető

Adjon meg egy egyszerű szótár alapú kódolást (a szótárral együtt) a

kikiriki

szóra.

kikiriki
k-1
i-2
r-3
ki-4
ik-5
kir-6
ri-7
iki-8

1,2,4,3,5

binárisan kódoltan nálam (5-ös a legmagasabb nálam)
1 -> 001
2 -> 010
3 -> 011
4 -> 100
5 -> 101

001 010 100 011 101

3,00 pont szerezhető

Az ismert egyenlőség/egyenlőtlenség felhasználásával,
pontosan válaszoljon arra a kérdésre, hogy a Golay-kód
hány hiba felismerésére és hány hiba javítására
alkalmas (tudjuk, hogy a kód hossza n=23 és d=7 a kódtávolság. (1+1 pont)

Teljesül az egyenlőség?
Ha igen, mit jelent ez a a kódrendszer javíthatósága szempontjából? (1 pont)

n=23, d=7, t=?

d=2t+1
7=2t+1
6=2t
t=3

d-1 hibát tud felismerni a Golay kód
6 hibát tud felismerni és 3 hibát tud javítani

Az egyenlőség teljesül 2t+1 = d, ami azt jelenti, hogy maximális javítóképességgel rendelkezik

◄ EGYÉNI PROJEKT-LEÍRÁSOK

Ugrás...